



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

A

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,258	05/22/2002	Joerg Schwenk	2345/172	9412
26646	7590	11/17/2005		
KENYON & KENYON ONE BROADWAY NEW YORK, NY 10004			EXAMINER HO, THOMAS M	
			ART UNIT 2134	PAPER NUMBER

DATE MAILED: 11/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/049,258	SCHWENK, JOERG	
	Examiner	Art Unit	
	Thomas M. Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 22 May 2002.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 9-16 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 9-16 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ . |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ . | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ . |

DETAILED ACTION

1. Claims 1-8 have been canceled.
2. Claims 9-16 are pending.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 9-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In particular, claim 9 recites the seed S may be derived deterministically by a trust center by linking only to a secret information v.

Additionally, the regeneration information is said to be “linked to the secret information v” in the last step of the claim.

However, the nature of this link is not disclosed in the claims. It would appear from the Specification that the Applicant intends this “linking” to mean “concatenating or combining with.” The Applicant however has not explicitly defined the term “linking”, but has rather appeared to provide an example of what it may comprise. If the Applicant desires it as such that “linking” consists of, or is equivalent to “concatenating” two values

together, a statement verifying this interpretation will overcome the current grounds of the 112 rejection over claim 9.

Claim 10 is rejected for the following reasons:

- the variables x, y, z lack antecedent basis. It appears that x and y are arguments for some mathematical relationship such as a function. Similarly it appears z is some value or output that arises as a result of the inputs x and y into the function k. If this is the case, the arguments need to be introduced in the same manner as the variables of claim 9.
- Applicant has recited the step “public parameter g known to the trust center and a secret key v available at the trust center are linked to a public key...” As stated previously, clarification of the term “linked” is required.
- The applicant has recited “c) from the knowledge of u, $k(u,v)$ and $k(u,w)$, in practice, one cannot infer $k(k(u,w)v);$ ”, however, the function $k(k(u,w)v)$ recites only a single argument for the function k. A comma is necessary to indicate that $k(u,w)$ and v are two different arguments, which the function $k(x,y) = z$ appears to necessitate.
- As a matter of form, the Examiner recommends clarifying the assignments and roles of the variables used throughout claim 10 and restructuring claim 10 so that it is more clear. For example, the applicant recites “public parameter g known to the trust center and a secret key v available at the trust center are linked to a public key $V=k(g,v)$ ”. The Examiner would recommend changing such a concise

assignment to read as follows “linked to a public key V wherein V is equal to $k(g,v)$.

The Examiner also recommends referring to the “key mapping” as “ $k()$ ” rather than k to clarify the distinction that k is a mathematical relationship, a function, rather than a variable.

Allowability

The Examiner has found the elements and steps of Applicant’s claims to be allowable save for a few informalities under which a rejection under 35 USC § 112 has been given. The Examiner’s search has uncovered US patent Gennaro et al. as the closest art of record. A reasons for allowance has not yet been given however due to the fact that the final allowance of these claims depends on how Applicant will amend or argue the claims and/or specification to overcome the 35 USC § 112 rejection.

Conclusion

4. The following art not relied upon is made of record:

- US patent 5937066, Gennaro et al. discloses a two-phase cryptographic recovery system invoking the generation of a key through a seed and is believed to be the closest art of record.

Art Unit: 2134

- US patent 5647000 Leighton discloses a failsafe key escrow system.
- US patent 4947430 discloses a blind digital signature system.

5. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist Telephone: 571-272-2100 Fax: 571-273-8300
Customer Service Representative Telephone: 571-272-2100 Fax: 571-273-8300

TMH

November 10th, 2005



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY AREA 2134
11/10/05